

REMARKS

The Office Action dated June 22, 2004 has been received and carefully noted. The above amendments to the specification and claims, and the following remarks, are submitted as a full and complete response thereto.

Applicant gratefully acknowledges the indication that claims 44-48 and 50-53 would be allowable if rewritten in independent form. It is respectfully submitted that these claims are allowable in their present form.

New claims 64-68 are added. Upon entry of this response, claims 33-68 will be pending in the present application. Claims 33 and 63-68 are independent claims. No new matter has been added. A Request for Continued Examination (RCE) is filed herewith. Claims 33-68 are respectfully submitted for consideration.

Claims 33-43, 49, 54-56, and 58-63 have been rejected under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 5,642,401 to Yahagi (Yahagi '401). This rejection is respectfully traversed.

Claim 33, upon which claims 34-43, 49, 54-56 and 58-62 depend, recites a method of securing communication between a first party and a second party in a telecommunications network. The method includes the step of defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The method also

includes the steps of selecting one of the plurality of different security methods in accordance with defined criteria and performing the security method.

Claim 63 recites a telecommunications network element for securing communication between a first party and a second party. The network element includes means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The network element also includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria and means for insuring that the communication between the first and second parties is in accordance with the selected security method.

Applicant respectfully submits that the claimed invention advantageously allows a relatively large number of different security methods to be implemented using only a small number of different messages. As shown at least in Figures 3 – 9, the claimed invention comprises a plurality of different security methods as recited in claims 33 and 63. Accordingly, claims 33 and 63 recite the feature of selecting a security method from a plurality of security methods. It is respectfully submitted that the references cited in the Office Action, taken either individually or in combination, fail to disclose or suggest the elements of any of the presently pending claims. Therefore, Applicant respectfully further submits that the references cited in the Office Action fail to provide at least the above-discussed non-obvious advantages of the claimed invention.

Yahagi '401 discloses an “authentication algorithm calculation means 6 [that] performs an authentication calculation by using an authentication random number sent from a base station 2 and the authentication key 5 as input parameters” (column 3, lines 63-67). In Figure 3 thereof, Yahagi '401 further discloses steps of a single authentication method. In Figure 4 thereof, Yahagi '401 discloses “an initial sequence which is started by a mobile station controller to cause a base station to generate a random number” (column 3, lines 38-40). In Figure 5 thereof, Yahagi '401 discloses “an initial sequence which is started by a data base to cause the base station to generate a random number” (column 3, lines 41-43). In Figure 6 thereof, Yahagi '401 discloses “pieces of information transferred between the respective constituent elements when there are two authentication targets” (column 3, lines 44-46).

Page 6 of the Office Action alleges that Yahagi '401 discloses an “authenticating technique based on a plurality of methods such as, generating random numbers (RAND (1-n), or SRES (1-n) between the network and the mobile station (figures 8 and 9, column 1 line 55 – column 2 line 23).” Applicant respectfully submits that this is a misinterpretation and/or misapplication of the phrase “plurality of methods” as recited in claims 33 and 63 and the specification. The cited portions of Yahagi '401 merely disclose, at best, a plurality of authentication steps of a single security method, and not a plurality of methods as recited in claims 33 and 63 of the present application.

The cited portions of Yahagi '401 (col. 2 lines 7-24) merely discloses a single security method, which is a function of a random number. Specifically, Yahagi '401

discloses that a single variable $RAND[j]$ changes and effects the authentication result SRES (i.e. $SRES = f(RAND[j])$). Hence, Yahagi '401 discloses a pair of values which are sent ($SRES[1...n]$, $RAND[1...n]$) i.e. a random value and the authenticated result based thereon. Yahagi '401 fails to even mention or suggest the feature of selecting a security method from a plurality of security methods as recited in claims 33 and 63. This point is further emphasized in portions of Yahagi '401 that discloses the use of a single security method. Specifically Yahagi '401 at col. 3 lines 63-67 states: "The authentication algorithm calculation means 6 performs an authentication calculation by using an authentication random number sent from a base station 2 and the authentication key 5 as input parameters." (emphasis added).

It is respectfully submitted that, Yahagi '401 fails to disclose or suggest at least the feature of "defining a criteria for selecting a one of a plurality of different security methods", as recited in claims 33 and 63 of the present application. The cited portions of Yahagi '401 also fails to disclose or suggest at least the above-discussed "defining" step, wherein "at least two different security methods [have] at least one message in common", as also recited in claims 33 and 63. It is further submitted that Yahagi '401 fails to even mention defining a criteria for selecting one of a plurality of different security methods. As discussed above, since Yahagi '401 fails to disclose or suggest a plurality of security methods, Yahagi '401 inherently fails to disclose defining a criteria for the selection of a method from a plurality of methods as recited in claims 33 and 63. Further, as discussed

above, Yahagi '401 fails to disclose or suggest at least "selecting one of the said plurality of different security methods", as recited in claims 33 and 63.

In addition, the Office Action alleges that Yahagi '401 at column 3 lines 1-27 discloses the step of selecting one of the said plurality of different security methods in accordance with said defined criteria and performing said security method. It is respectfully submitted that Yahagi '401 merely discloses that the security method is based on a random number and on an authentication key variable. However, Yahagi fails to even mention selecting between this security method and any other security method, much less defining a criteria for selecting between the different security methods, as recited in claims 33 and 63.

Applicant respectfully submits that Figures 3-9 of the present application illustrate various different examples of the "plurality of different security methods" recited in claims 33 and 63 of the present application. Applicant also respectfully submits that, as disclosed in the specification of the present application, the "criteria for selecting one of a plurality of different security methods" recited in claims 33 and 63 may include, for example, the processing capability of each of the two parties, or the time since the last security method was performed, as well as a random selection. Applicant further points out that, as recited in claims 33 and 63, "at least two different security methods [have] at least one message in common".

As discussed above, Yahagi '401 discloses only the single security method illustrated in Figure 3. Applicant also points out that column 2 lines 7-24 and column 3

lines 1-17 of Yahagi '401, at best, merely disclose a single security method that utilizes a plurality of authentication random numbers and corresponding authentication calculation results. However, Applicant respectfully submits that these random numbers and calculation results are no more than messages in the authentication method illustrated in Figure 3 of Yahagi '401. Hence, at least in view of the above, Applicant again points out that Yahagi '401 fails to disclose or suggest at least the "defining" and "selecting" steps recited in claim 33, or the "means for defining" and "selection means" recited in claim 63 of the present application.

At least in view of the above, Applicant respectfully submits that Yahagi '401 fails to disclose or suggest the subject matter recited in claims 33 and 63 of the present application. Hence, Applicant further submits that claims 33 and 63 are patentable over Yahagi '401 at least for the reasons discussed above.

As mentioned above, claims 34-43, 49, 54-56, and 58-62 depend upon claim 33. Therefore, these claims inherit all of the patentable distinctions thereof. Hence, Applicant respectfully submits that claims 34-43, 49, 54-56, and 58-62 are patentable over Yahagi '401 at least for the reasons discussed above in connection with claim 33.

At least in view of the above remarks, reconsideration and withdrawal of the rejection of claim 33-43, 49, 54-56, and 58-63 under 35 U.S.C. § 102(b) as being anticipated by Yahagi '401 is respectfully requested.

Claim 57 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Yahagi '401 in view of U.S. Patent No. 5,537,474 to Brown et al. (Brown '474).

Although it is acknowledged in the Office Action that Yahagi '401 fails to disclose that the exchange of messages between two parties permits a shared secret to be created, which is used to authenticate the communication between the parties, it is alleged in the Office Action that Brown '474 discloses such an exchange. It is further alleged that Brown '474 may be combined with Yahagi '401 to produce the subject matter recited in claim 57. This rejection is respectfully traversed.

Brown '474, at least in the title thereof, discloses a "method and apparatus for authentication in a communication system". Brown '474 also discloses "a temporary shared secret data key (SSD) for use in authentication and encryption" (column 4, lines 23-24).

However, Brown '474 fails to make up for the deficiencies of Yahagi '401 with respect to claim 33. Hence, at least since claim 57 depends upon claim 33 and thereby inherits all of the patentable distinctions thereof, Applicant respectfully submits that claim 57 is patentable over Yahagi '401 and Brown '474, taken either individually or in combination, at least for the reasons discussed above in connection with claim 33.

At least in view of the above remarks, reconsideration and withdrawal of the rejection of claim 57 under 35 U.S.C. § 103(a) over Yahagi '401 in view of Brown '474 is respectfully requested.

Applicant gratefully acknowledges the indication that claims 44-48 and 50-53 would be allowable if rewritten in independent form. As discussed above, it is

respectfully submitted that these claims are allowable in their present form. Accordingly, withdrawal of the objection of claims 44-48 and 50-53 is respectfully requested.

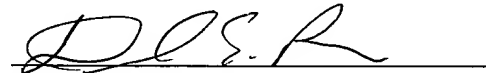
Applicant respectfully submits that new independent claims 64-68 recite subject matter that is neither disclosed nor suggested in the cited references at least for the reasons discussed above regarding independent claims 33 and 63. Specifically, the cited references fail to disclose or suggest the feature of a plurality of different security methods as recited in claims 64-68. Applicant respectfully submits that claims 64-68 are in condition for allowance.

Applicant respectfully submits that all of the comments included in the Office Action have been addressed and that all of the objections and rejections included in the Office Action have been overcome. Hence, Applicant respectfully further submits that, at least in view of the above, claims 33-68 of the present application contain allowable subject matter. Therefore it is respectfully requested that all claims pending in the present application be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown

Registration No. 51,091

Customer No. 32294

SQUIRE, SANDERS & DEMPSEY LLP

14TH Floor

8000 Towers Crescent Drive

Tysons Corner, Virginia 22182-2700

Telephone: 703-720-7800

Fax: 703-720-7802

DEB:mm

Enclosures: Petition for Extension Time
Amendment Transmittal
Request for Continued Examination